POLICY

Enterprise Terms of Service

Contract-grade terms for NHS / enterprise procurement and ISO 27001 supplier assurance

DOCUMENT TYPE	Policy
VERSION	1.0 · Effective 12 December 2025
OWNER	Remote-I Ltd — Technical Lead
CLASSIFICATION	Internal / Customer Assurance
REVIEW CYCLE	Annual, and after major storage/schema change or incident

ORGANISATION

LEGAL ENTITY	Remote-I Ltd
COMPANY NUMBER	15293974
REGISTERED OFFICE	45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB
COMPLIANCE CONTACT	compliance@remote-i.com
DATA PROTECTION LEAD	Remote-I Ltd — Data Protection Lead

These Terms of Service ("**Terms**") govern access to and use of the Remote-I software platform and related services (the "**Platform**" or "**Services**") provided by Remote-I Ltd.

By creating an account, executing an Order Form (as defined below), or otherwise accessing or using the Platform, you agree to these Terms. If you are accepting these Terms on behalf of a hospital, imaging centre, radiology provider, or other organisation, you represent that you are authorised to bind that organisation.

> **These Terms are written for use in hospital procurement, NHS DSP Toolkit governance, ISO 27001 supplier assurance, grant due diligence, and enterprise partner review. They are intended to be contract-grade, but you should still have them reviewed by your legal counsel before signing with NHS Trusts or enterprise partners.**

1. Definitions and Interpretation

1.1 Definitions

In these Terms:

- **"Account"** means a user account created for an Authorised User to access the Platform.
- **"Affiliate"** means any entity that controls, is controlled by, or is under common control with a party.
- **"Authorised Users"** means individuals authorised by Customer to access the Platform, including Hospital Users and (where applicable) Radiographers, Administrators, and other staff.
- **"Availability"** means the ability to access the Platform over the public internet excluding Permitted Downtime.
- **"Confidential Information"** has the meaning set out in Section 12.
- **"Controller", "Processor", "Personal Data", "Processing"** have the meanings in UK GDPR / GDPR.
- **"Customer"** means the organisation (e.g., hospital, imaging centre, radiology provider) that subscribes to or pilots the Platform.
- **"Customer Data"** means all data (including Personal Data) submitted, stored, sent, or otherwise processed via the Platform by or on behalf of Customer, including job information, workforce metadata, SOP content, compliance documents, incident entries, and audit events.
- **"Documentation"** means user guides, policies, and instructions made available by Remote-I describing the Platform and its use.
- **"DPA"** means the Data Processing Agreement between Remote-I and Customer governing Processing of Personal Data on Customer's behalf.
- **"Hospital User"** means a Customer Authorised User acting in a hospital / clinical governance capacity (e.g., manager, admin, scheduler, HR / compliance).
- **"Order Form"** means a written ordering document or subscription agreement referencing these Terms that specifies Subscription Plan, fees, and term, signed or accepted by Customer.
- **"Pilot"** means a time-limited evaluation deployment under a Pilot Order Form or pilot addendum.
- **"Permitted Downtime"** means planned maintenance windows, emergency maintenance, outages caused by Customer systems or third parties outside Remote-I's control, and events of Force Majeure.
- **"Radiographer"** means an individual user of the Platform who provides radiography services and uses the Platform to manage availability, compliance documentation, SOP acknowledgements, and job workflows.
- **"SOP"** means a standard operating procedure or policy uploaded by or on behalf of Customer, including protocols requiring acknowledgement and/or sign-off.
- **"Subscription Plan"** means the commercial plan selected by Customer, including any Pilot or paid subscription plan.

1.2 Interpretation

Headings are for convenience only and do not affect interpretation. "Including" means "including without limitation".

2. Contract Structure and Order of Precedence

2.1 Contract Components

This contract may consist of:

- the Order Form;
- these Terms;
- the DPA (if applicable);
- any mutually signed addenda (e.g., Pilot addendum, SLA addendum).

2.2 Precedence

> **If there is a conflict, precedence is: Order Form DPA Addenda Terms Documentation.**

3. Scope of Services

3.1 What Remote-I Provides

Remote-I provides the Platform as a hosted SaaS solution which (subject to the Subscription Plan) may include the functionality described in Annex 2 (Service Description), including:

- workforce and role-based user management;
- job / shifts creation, assignment, acceptance, lifecycle tracking and handover workflows;
- radiographer availability and preference management;
- compliance documentation capture and tracking (e.g., right-to-work, registration evidence, insurance evidence, training evidence);
- SOP publishing, acknowledgement / signature capture, and audit trail;
- incident reporting and reflection workflows;
- internal messaging / job chat (where enabled);
- notifications (email / SMS where enabled);
- governance reporting and exports (where enabled).

3.2 What Remote-I Does Not Provide

Remote-I does not:

- provide diagnostic reporting or clinical interpretation;
- provide medical advice or clinical decision support;
- replace RIS / PACS systems or act as a modality console;
- guarantee staffing levels, radiographer availability, or clinical outcomes;
- verify the authenticity of professional credentials unless explicitly agreed as a managed verification service in the Order Form.

3.3 Intended Use and Data Minimisation

The Platform is designed primarily for workforce operations and governance. Customer shall ensure users do not input unnecessary patient-identifiable data into the Platform. Where Customer elects to store or transmit patient-identifiable information through the Platform, Customer is responsible for ensuring (i) lawful basis and transparency, (ii) appropriate security controls, and (iii) that such processing is covered by the DPA and any additional safeguards required by law.

4. Eligibility, Accounts, and Access Control

4.1 Account Creation

Authorised Users must provide accurate, complete, and current registration information. Remote-I may require email verification and may support multi-factor authentication (MFA).

4.2 Authorised User Management

Customer is responsible for:

- authorising and de-authorising users;
- ensuring role assignments follow “least privilege”;
- promptly revoking access for leavers or role changes;
- ensuring no account sharing occurs.

4.3 Credentials and MFA

Customer and Authorised Users must:

- keep credentials confidential;
- use strong passwords;
- enable MFA where available and required by Customer policy or Remote-I security settings;
- promptly notify Remote-I of suspected compromise.

4.4 Security of Endpoints

Customer is responsible for ensuring any devices used to access the Platform (including hospital-managed endpoints) meet basic security requirements (up-to-date OS, malware protection, device access controls), especially for privileged accounts.

5. Customer Obligations (Hospitals / Imaging Centres)

Customer shall:

5.1 Use of the Platform

Use the Platform only for lawful purposes and in accordance with these Terms, Documentation, and applicable clinical governance standards.

5.2 Accuracy and Integrity of Customer Data

Ensure that job postings, SOP content, compliance requirements, and workflow data are accurate and maintained. Customer is responsible for the content and legality of Customer Data.

5.3 Credentialing and Clinical Governance

Customer remains solely responsible for:

- verifying that radiographers are suitably qualified, registered, competent, and authorised under local policies;
- local induction, training, supervision, and scope-of-practice;
- clinical governance frameworks, incident management, and escalation;
- ensuring the Platform is configured to reflect Customer's governance requirements (SOPs, approval steps, job rules).

5.4 Policy Enforcement

Customer is responsible for ensuring Authorised Users comply with:

- confidentiality obligations;
- acceptable use rules;
- SOP requirements;
- local IT and IG policies (including NHS DSP Toolkit-aligned controls where applicable).

6. Radiographer Obligations (Where Applicable)

Radiographers shall:

6.1 Accuracy of Professional Information

Provide accurate and current professional details and compliance documents (e.g., registration details, proof of right-to-work, insurance, training evidence).

6.2 SOP Compliance

Review and acknowledge SOPs and protocols required by Customer prior to undertaking work.

6.3 Professional Conduct

Use the Platform in good faith; do not misrepresent credentials; do not misuse messaging; comply with relevant clinical governance processes and lawful instructions.

7. Acceptable Use, Prohibited Conduct, and Content Standards

Customer and Authorised Users shall not:

- attempt to gain unauthorised access to systems or data;
- circumvent authentication, security controls, or audit logging;
- introduce malware, exploit vulnerabilities, or perform scanning;
- upload unlawful, infringing, defamatory, or harmful content;
- upload patient-identifiable data contrary to Customer instructions or lawful basis;
- use the Platform to send spam, harassment, or abusive messages;
- reverse engineer, copy, or create derivative works of the Platform except as permitted by law.

Additional rules are set out in **Annex 1 (Acceptable Use Policy)**.

8. Service Levels, Support, and Maintenance

8.1 Support

Remote-I will provide support according to the Subscription Plan and Annex 3 (Support & Availability Targets). Support may include issue triage, bug fixes, and platform guidance.

8.2 Maintenance

Remote-I may perform planned maintenance. Where reasonably practicable, Remote-I will provide advance notice for scheduled maintenance that may impact Availability.

8.3 No Guaranteed Uptime Unless Agreed

Any binding SLA must be agreed in the Order Form or an SLA addendum. Otherwise, Availability is provided on a commercially reasonable basis.

9. Security, Auditability, and Assurance

9.1 Security Measures

Remote-I will implement and maintain appropriate technical and organisational measures ("TOMs") to protect Customer Data against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures are described in the DPA and may include:

- access controls and role separation;
- MFA support;
- encrypted transport (TLS) for data in transit;
- audit trails for key actions;
- secure backup processes and restore procedures;
- segregation of sensitive configuration and credentials.

9.2 Logging and Audit Trails

Remote-I records audit events to support governance, investigations, and compliance. Customer acknowledges that audit logs are security-relevant and may be retained for defined periods to support accountability.

9.3 Customer Audit Rights

Where required for regulated environments (e.g., NHS, ISO assessment), Customer may request reasonable assurance information (e.g., security policy summaries, penetration testing summaries where available, incident response procedures), subject to confidentiality and reasonable limits. Any on-site audit rights must be agreed in writing and shall not compromise security or other customers' confidentiality.

9.4 Vulnerability Handling

Remote-I will maintain a vulnerability management process proportionate to the Platform's risk profile, including prioritisation and remediation for critical issues within reasonable timeframes.

10. Data Protection (GDPR / UK GDPR)

10.1 Roles

Customer is generally the Controller of Customer Data processed via the Platform. Remote-I is generally the Processor for such Customer Data, and is a Controller for its own corporate and account-administration data (e.g., billing contacts, platform security logs for its legitimate interests), as described in the Privacy Policy and DPA.

10.2 DPA Incorporation

Where Remote-I processes Personal Data on behalf of Customer, the parties agree to the DPA which is incorporated by reference and forms part of this contract.

10.3 Customer Instructions

Customer shall ensure that any Processing instructions are lawful and documented, and that it has provided required privacy notices and obtained any consents required by law.

10.4 Special Category Data

The Platform is not intended for routine processing of special category patient data. If Customer uses the Platform to process such data, Customer must ensure appropriate safeguards (including DPIA where applicable) and confirm DPA coverage and required transfer mechanisms.

11. Confidentiality

11.1 Confidential Information

"Confidential Information" includes any non-public information disclosed by one party to the other relating to business, operations, technology, security, Customer Data, or clinical governance processes, including the Platform itself and Documentation.

11.2 Obligations

Each party shall:

- use the other's Confidential Information only for performing obligations and exercising rights under this contract;
- restrict disclosure to personnel with a need to know;
- protect Confidential Information using no less than reasonable care.

11.3 Exceptions

Confidentiality obligations do not apply to information that is:

- publicly known without breach;
- independently developed without reference;
- lawfully received from a third party;
- required to be disclosed by law, provided that (where permitted) the disclosing party is notified.

12. Intellectual Property and Feedback

12.1 Platform Ownership

Remote-I owns all intellectual property rights in the Platform, including software, UI, workflows, Documentation, and related materials.

12.2 Licence to Customer

Subject to payment of fees (if any) and compliance with these Terms, Remote-I grants Customer a limited, non-exclusive, non-transferable, revocable licence for Authorised Users to access and use the Platform during the subscription term for Customer's internal business purposes.

12.3 Customer Data Ownership

Customer retains ownership of Customer Data. Customer grants Remote-I a licence to host, process, transmit, and display Customer Data solely to provide the Services and fulfil obligations under this contract.

12.4 Feedback

If Customer or users provide feedback, Remote-I may use it without restriction to improve the Platform, without obligation to compensate, provided Remote-I does not disclose Customer Confidential Information in doing so.

13. Third-Party Services and Subprocessors

13.1 Third-Party Services

The Platform may rely on third-party services (e.g., hosting, email, SMS). Remote-I is not responsible for outages or failures caused by third parties beyond its reasonable control, but will use commercially reasonable efforts to mitigate.

13.2 Subprocessors

Remote-I may appoint subprocessors to deliver the Services. Subprocessor obligations and notification are governed by the DPA.

14. Fees, Billing, and Taxes

14.1 Fees

Fees (if any) are as set out in the Order Form or Subscription Plan. Radiographer accounts may be free, while Customer accounts may be paid; the commercial model is defined in the Order Form.

14.2 Invoicing and Payment

Payment terms, billing cycles, and invoicing are defined in the Order Form. Overdue payments may result in suspension following reasonable notice.

14.3 Taxes

Fees are exclusive of VAT or sales taxes unless stated otherwise.

15. Pilots, Beta Features, and Evaluation Use

15.1 Pilot Terms

If Customer is using the Platform under a Pilot, then:

- features may change;
- performance targets may be "best effort" unless stated;
- Remote-I may collect enhanced feedback and usage analytics for improvement;
- the Pilot may be terminated by either party on notice as stated in the Order Form or pilot addendum.

15.2 No Clinical Reliance Without Governance

Customer must not rely on the Platform as a clinical safety control. The Platform is a governance and workflow tool and does not replace clinical supervision, local protocols, or vendor modality safeguards.

16. Warranties and Disclaimers

16.1 Mutual Authority

Each party warrants it has authority to enter into and perform this contract.

16.2 Service Warranty

Remote-I warrants it will provide the Services with reasonable skill and care consistent with a SaaS provider in a regulated environment.

16.3 Disclaimers

Except as expressly stated, the Platform is provided "as is". Remote-I does not warrant uninterrupted availability, error-free operation, or that the Platform will meet all Customer requirements unless specified in the Order Form.

Remote-I does not provide clinical advice, diagnosis, or medical device functionality. Customer remains responsible for clinical decisions and governance.

17. Indemnities

17.1 IP Infringement Indemnity

Remote-I will defend Customer against third-party claims that the Platform infringes UK intellectual property rights, and will pay damages finally awarded or agreed in settlement, provided Customer:

- promptly notifies Remote-I;
- cooperates;
- allows Remote-I to control defence and settlement.

Remote-I may (at its option) modify the Platform to avoid infringement, procure a licence, or terminate affected Services and refund prepaid unused fees.

17.2 Customer Indemnity

Customer will indemnify Remote-I against claims arising from:

- Customer Data content;
- Customer's unlawful use;
- breach of confidentiality or data protection obligations by Customer;
- unauthorised use by Customer's Authorised Users.

18. Limitation of Liability

18.1 Excluded Losses

Neither party is liable for indirect, consequential, or special damages, including loss of profits, loss of revenue, loss of business, or loss of goodwill.

18.2 Liability Cap

Each party's aggregate liability arising out of or related to the Services is limited to the fees paid by Customer in the 12 months preceding the event giving rise to liability (or £10,000 if fees are zero in a Pilot), except for excluded categories below.

18.3 Unlimited / Non-Excluded Liability

Nothing limits liability for:

- death or personal injury caused by negligence;
- fraud or fraudulent misrepresentation;
- liability that cannot be limited under law;
- breach of confidentiality (cap may be agreed in Order Form);
- data protection liabilities (handled per DPA and applicable law).

19. Term, Suspension, and Termination

19.1 Term

These Terms begin on acceptance and continue until terminated in accordance with the Order Form or these Terms.

19.2 Suspension

Remote-I may suspend access (in whole or part) if:

- Customer's use presents security risk;
- unlawful activity is suspected;
- fees are overdue;
- required to do so by law.

Remote-I will use reasonable efforts to notify Customer and restore service promptly after the issue is resolved.

19.3 Termination for Cause

Either party may terminate for material breach not cured within 30 days of notice (or shorter where breach is incapable of cure or involves security).

19.4 Termination for Convenience

Termination rights for convenience (and notice periods) must be stated in the Order Form.

20. Data Return, Deletion, and Exit Support

20.1 Data Export

Upon termination, Customer may request export of Customer Data in a standard format where technically feasible, subject to reasonable charges if not included in the Subscription Plan.

20.2 Deletion

Remote-I will delete Customer Data after termination in accordance with the DPA, subject to legal retention requirements and reasonable backup retention cycles.

20.3 Transition Assistance

If requested, Remote-I may provide transition assistance (data exports, configuration handover) at professional services rates unless included in the Order Form.

21. Changes to the Platform and Terms

21.1 Platform Updates

Remote-I may update the Platform to improve security, performance, or functionality. Remote-I will not materially reduce core functionality during a paid term without reasonable notice and a reasonable alternative / remedy.

21.2 Changes to Terms

Remote-I may update these Terms. For paid subscriptions, changes will generally apply at renewal unless a change is required by law or for security.

22. Force Majeure

Neither party is liable for failure to perform due to events beyond reasonable control (e.g., major outages, natural disasters, war, labour disputes, government action). The affected party will notify the other and take reasonable steps to mitigate.

23. Assignment and Subcontracting

Customer may not assign this contract without Remote-I's prior written consent (not to be unreasonably withheld). Remote-I may assign to an Affiliate or in connection with a merger or sale of assets. Remote-I may subcontract performance subject to the DPA and confidentiality obligations.

24. Notices

Notices must be in writing and sent to the relevant party's registered office or compliance email, unless otherwise specified in the Order Form.

Remote-I notice email: **compliance@remote-i.com**.

25. Governing Law and Jurisdiction

These Terms are governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction, unless the Order Form specifies otherwise.

26. Entire Agreement; Severability; Waiver

This contract constitutes the entire agreement regarding its subject matter and supersedes prior discussions. If any provision is unenforceable, the remainder remains effective. Failure to enforce a right is not a waiver.

ANNEX 1

Acceptable Use Policy

Prohibited conduct on the Remote-I Platform

Customer and Authorised Users must not:

- attempt to access data belonging to another customer or user without authorisation;
- probe, scan, or test vulnerability of the Platform without written permission;
- bypass security controls or attempt privilege escalation;
- upload malicious code, ransomware, spyware, or any harmful payload;
- use the Platform for harassment, discrimination, or unlawful communications;
- upload patient-identifiable data unless Customer has lawful basis and explicitly permits it; minimise any such data and avoid free-text entry of patient identifiers;
- use the Platform to store or transmit highly sensitive clinical records as a substitute for approved clinical systems;
- reverse engineer, copy, scrape, or mirror the Platform (except where legally permitted);
- interfere with service availability, performance, or integrity.

> **Remote-I may suspend accounts that breach this AUP.**

ANNEX 2

Service Description

Functional detail of Platform modules

The Platform may include the following modules (subject to Subscription Plan and configuration):

A. User and Role Management

- Hospital user accounts, roles, permissions
- Radiographer accounts and role separation
- MFA support for privileged users
- Email verification / account status controls

B. Job / Shift Lifecycle Management

- Job creation (time, location, modality context, notes)
- Assignment to radiographer or pool
- Acceptance / decline logic
- Status lifecycle tracking (created accepted in progress completed handover)
- Handover workflows for governance continuity
- Export capability (CSV / XLS / ICS where enabled)

C. Compliance & Credentialing

- Profile fields for qualifications and identifiers
- Document upload and storage (e.g., DBS, insurance, right-to-work, training)
- Expiry tracking and reminders (where configured)
- Hospital-side review and metadata tags

D. SOP Management and Acknowledgement

- Upload and publish SOPs per organisation
- Radiographer access and acknowledgement
- SOP sign-off records (who / when / version)
- Audit logging for governance evidence

E. Incidents and Reflection

- Incident capture with classification
- Reflection notes
- Governance export / reporting where enabled
- Audit logs of incident lifecycle

F. Messaging and Notifications

- Job chat / messaging within the platform (where enabled)

- Email notifications (SMTP via configured provider)
- SMS notifications (via configured gateway)
- Logging of notification attempts (without exposing sensitive message content in technical logs)

G. Audit and Reporting

- Audit log of key platform actions (auth events, job lifecycle, SOP acknowledgements, admin actions)
- Audit report generation where enabled

ANNEX 3

Support & Availability Targets

Non-binding unless included in the Order Form

Unless a binding SLA is included in the Order Form:

- **Target Availability:** commercially reasonable; planned maintenance excluded.
- **Support channel:** email to support / compliance contact (as specified).

Response targets (best effort)

Severity	Description	Initial response
S1	System down	4 business hours
S2	Major feature impaired	1 business day
S3	Minor issue	3 business days

Security incidents: prioritised per Incident Response Policy and DPA.

End of Enterprise Terms of Service. For enquiries, contact compliance@remote-i.com.